WEB SECURITY

Config server firewall(csf)

MARTIN NJAU
Systems Administrator
mnjau@kenet.or.ke

27th October 2015

Some Material Borrowed
From: NSRC

kenet
Kenya Education Network

NSRC
Network Startup Resource Center

Introduction

- Config Server Firewall (or CSF) is a free and advanced firewall for most Linux distributions.
- In addition to the basic functionality of a firewall – filtering packets – CSF includes other security features, such as login/intrusion/flood detections. CSF includes UI integration for cPanel, DirectAdmin and Webmin.
- CSF is able to recognize many attacks, such as port scans, SYN floods, and login brute force attacks on many services. It is configured to temporarily block clients who are detected to be attacking the cloud server.

Login authentication failure daemon:

- CSF checks the logs for failed login attempts at regular time interval, and is able to recognize most unauthorized attempts to gain access to your cloud server.
- You can define the desired action CSF takes and after how many attempts in the configuration file.
- Enable LDF DAEMON:
- #vi /etc/csf/csf.conf
- LF_DAEMON = "1"
- The following applications are supported by this feature:
- -

Cont...

- Courier imap, Dovecot, uw-imap, Kerio
- openSSH
- cPanel, WHM, Webmail (cPanel servers only)
- Pure-ftpd, vsftpd, Proftpd
- Password protected web pages (htpasswd)
- Mod_security failures (v1 and v2)
- Su host failures
- Exim SMTP AUTH

Process tracking

- CSF can be configured to track processes in order to detect suspicious processes or open network ports, and send an email to the system administrator if any is detected. This may help you to identify and stop a possible exploit on your web server

Directory watching

- Directory watching monitors the /temp and other relevant folders for malicious scripts, and sends an email to the system administrator when one is detected.

Messenger service

- Enabling this feature allows CSF to send a more informative message to the client when a block is applied. This feature has both pros and cons. On one hand, enabling it provides more information to the client, and thus may cause less frustration for instance in case of failed logins. On the other hand, this provides more information, which might make it easier for an attacker to attack your web server.

Port flood protection

- This setting provides protection against port flood attacks, such as denial of service (DoS) attacks. You may specify the amount of allowed connections on each port within time period of your liking. Enabling this feature is recommended, as it may possibly prevent an attacker forcing your services down. You should pay attention to what limits you set, as too restrictive settings will drop connections from normal clients. Then again, too permissive settings may allow an attacker to succeed in a flood attack.

Connection limit protection

- This feature can be used to limit the number concurrent of active connections from an IP address to each port. When properly configured, this may prevent abuses on the server, such as DoS attacks.

Port/IP address redirection

- CSF can be configured to redirect connections to an IP/port to another IP/port. Note: After redirection, the source address of the client will be the server's IP address. This is not an equivalent to network address translation (NAT).

IP block lists

- This feature allows CSF to download lists of blocked IP addresses automatically from sources defined by you.

Basic Configuration

- CSF can be configured by editing its configuration file csf.conf in /etc/csf:
- Vi /etc/csf/csf.conf
- The changes can be applied with command:
- #csf -r
- Enabling the Csf firewall:
- change TESTING = "1" to TESTING = "0"

Configuring ports

- The ports opened by default are the following:
- TCP_IN="20,21,22,25,53,80,110,143,443,465,587,993,995"
- TCP_OUT = "20,21,22,25,53,80,110,113,443"
- UDP_IN = "20,21,53"
- UDP_OUT = "20,21,53,113,123

Additional settings

- ICMP_IN Setting ICMP_IN to 1 allows ping to your server and 0 refuses are such requests. If you are hosting any public services, it is recommended to allow ICMP requests, as these can be used to determine whether or not your service is available.
- ICMP_IN_LIMIT Sets the number of ICMP (ping) requests allowed from one IP address within a specified amount of time. There is usually no need to change the default value (1)
- DENY_IP_LIMIT Sets the number of blocked IP addresses CSF keeps track of. It is recommended to limit the number of denied IP addresses as having too many blocks may slow down the server performance.

Cont...

- SYNFLOOD, SUNFLOOD_RATE and SYNFLOOD_BURST This offers protection against SYN flood attacks. This slows down the initialization of every connection, so you should enable this only if you know that your server is under attack.
- CONNLIMIT Limits the number of concurrent active connections on port.
- Value: 22;5;443;20
- This would allow 5 concurrent connections on port 22 and 20 concurrent connections on port 443.

Cont..

- PORTFLOOD Limits the number of connections per time interval that new connections can be made to specific ports.
- Value: 22;tcp;5;250
- This would limit block the IP address if more than 5 connections are established on port 22 using TCP protocol within 250 seconds. The block is removed once 250 seconds have passed after the last packet sent by the client to this port

Blocking and Allowing IP Addresses

- One of the most basic features of a firewall is the ability to block certain IP address.
- If you would like to block an IP address or range, open csf.deny.
- #vi /etc/csf/csf.deny
- you should add the following lines to the file:
- x.x.x.x
- y.y.y.y/24

- #csf -d 11.22.33.44

Allowing IP addresses

- If you would like an IP address or range to be excluded from all blocks and filters, you may add them to csf.allow file.
- note that allowed IP addresses are allowed even if they are explicitly blocked in csf.deny file.
- Allowing IP addresses works similarly to blocking them. The only difference is that you should edit /etc/csf/csf.allow instead of csf.deny
- To allow IP address that has already been blocked use:
- #csf -dr 11.22.33.44

Ignoring IP addresses

- CSF also offers ability to exclude IP addresses from the firewall filters. IP addresses in csf.ignore will bypass the firewall filters, and can only be blocked if listed in csf.deny fille.
- Edit /etc/csf/csf.ignore file.
- #vi /etc/csf/csf.ignore

Q&A.

?

kenet

Kenya Education Network

THANK YOU!